QUANTIFIND



Crypto Convergence Summary Report

Rethinking Compliance in the Age of Digital Assets

JULY 16, 2025

Event Overview

As adoption of digital assets accelerates, so too does the complexity of associated financial crime. From ransomware to sanctions evasion, threat actors are exploiting crypto's speed, pseudonymity, and global reach. Traditional approaches to risk management are struggling to keep up.

At our recent Crypto Convergence event, hosted by Quantifind in partnership with Deloitte, Elliptic, and ManchesterCF, leaders from financial services, crypto-native firms, law enforcement, and regulatory agencies came together to explore how to detect and disrupt crypto-related illicit finance.

We extend our sincere thanks to all participants for your insights and candor. The conversations spanning governance, data, AI, and regulation surfaced practical strategies and emerging imperatives for safeguarding the evolving digital asset ecosystem. This report summarizes the key takeaways from the event.

PANEL SUMMARY

Investing in Compliance Amid Rapid Crypto Evolution

The panel featured experts from OKX, PayPal Digital, Paul, Weiss, and FINRA. Together, they examined how institutions are adapting their compliance programs to address new risks, bridge regulatory uncertainty, and position crypto for long-term success.

Key Themes and Insights

Investment in Compliance Maturity

- Crypto exchanges are significantly scaling their compliance operations, with a substantial portion of their organizations now dedicated to risk management.
- Digital banks emphasize embedding crypto oversight within traditional financial control frameworks, including board governance, enterprise risk, and the three lines of defense.

Major Pain Points: Identity and Sanctions

- High-speed, borderless transactions and pseudonymity complicate the process of sanctions screening and identity verification.
- Alert volumes spike when analytics vendors flag previously unattributed wallets—often overwhelming operations teams.
- Cross-border data flow and lack of geolocation controls create friction in applying traditional compliance standards.

Regulatory Landscape and Expectations

- FINRA continues in an advisory role, preparing for a more prescriptive regulatory framework.
- Regulators expect crypto firms to act proactively, leveraging available data, documenting controls, and demonstrating risk-based decisions—even in the absence of specific rules.

Public–Private Collaboration

- Firms that engage early with regulators and share intelligence (e.g., wallet clusters) are better positioned for long-term credibility and trust.
- Regulators emphasized the need for crypto-native firms to operate with the same rigor as traditional financial institutions.

Evolving Technology and Investigative Approaches

- AI and knowledge graphs are transforming transaction monitoring from rule-based alerts to relationship-based risk assessments.
- Leading firms are shifting toward entity-centric investigations, supported by more technical staff and explainable AI models.
- Governance, model validation, and internal education (e.g., AI certifications) are crucial to the responsible deployment of AI.

Build vs. Buy: Crypto's Tech-Forward Approach

- Crypto firms tend to build compliance tooling in-house to better integrate across platforms and blockchain analytics tools.
- A noted best practice is to ring-fence compliance engineering from product teams to preserve independence and auditability.

©2025 Quantifind, Inc.

ROUNDTABLE SUMMARY

Emerging Risks and Control Gaps

In facilitated discussions, participants addressed current crypto-related risks, such as scams, sanctions evasion, and stablecoins, and shared ideas to enhance detection and control.

Behavioral Patterns in Scams

Participants emphasized that many scams, especially romance, refund, and account takeover frauds, follow predictable yet increasingly industrialized patterns:

- Small initial deposits followed by large, rapid outgoing transfers and fund splitting.
- Fake “refunds” used to legitimize scam activity and confuse operations teams.
- Coaching victims through KYC or fraud checks using prewritten scripts.
- High-velocity transfers that often outpace daily monitoring cycles.
- Scams targeting older adults who open new accounts with large deposits.
- Use of shared devices or “scam compounds” in Southeast Asia, where large teams create and operate multiple accounts from racks of phones and tablets.

Stablecoins and Sanctions Evasion

Stablecoins remain the preferred tool for transferring funds across jurisdictions due to their price stability and liquidity. Key red flags and concerns include:

- Test deposits and rapid swapping to/from privacy coins.
- Use of VPNs, mismatched geolocation data, and spoofed device IDs.
- Low transparency and light-touch controls by stablecoin issuers—many rely on intermediaries and lack enforceable minting and burning oversight.
- Jurisdictional arbitrage via stablecoin APIs and lax regulatory environments.

©2025 Quantifind, Inc.

Control Gaps and Detection Weaknesses

Participants identified several systemic weaknesses:

- **Fragmented compliance functions** (fraud, KYC, AML, sanctions) that inhibit unified risk detection.
- **Entity resolution challenges**, especially across wallet addresses and behavior patterns.
- **Staffing shortages** in areas like forensic accounting and token intelligence.
- **Overreliance on attestations** rather than independent audits for stablecoin reserves.
- **Jurisdictional fragmentation**, where differing regulatory regimes limit internal data sharing, create compliance silos, and introduce inconsistent oversight—even within the same country or region.
- **Lack of real-time collaboration** between financial institutions and with law enforcement, which remains mostly retroactive.
- **Perceived privacy concerns** that are often misunderstood but continue to inhibit stronger detection methods and public trust.

Stablecoins and Sanctions Evasion

Participants shared a range of observable indicators that could improve onboarding and monitoring efforts:

- Shared or recycled KYC selfie images.
- Evidence of third-party coaching during liveness checks.
- Sudden changes in account behavior, device, or location patterns.
- Cross-platform associations with flagged wallets or token projects.
- Use of dark web or Tor traffic (with caution due to false positives).
- Behavioral signals such as frequent late-night logins, unusual sweep-like transfers in specific jurisdictions, or structuring behaviors tailored to crypto protocols.

CONCLUSION

Final Thoughts and Next Steps

Crypto-native firms are under pressure, but also uniquely positioned to redefine how compliance operates in a digital-first financial system. The Crypto Convergence event revealed that leading institutions are not waiting for regulation to catch up. They are:

- Building AI-assisted, entity-centric compliance models.
- Elevating compliance to the board level.
- Investing in knowledge-sharing and technical skill development.
- Driving transparency with explainable AI, robust governance, and proactive regulator engagement.

We are grateful for your contributions. Your insights will shape Quantifind's crypto risk solutions, partnerships, and future convenings. If you'd like to stay engaged through follow-ups, pilots, or future events please don't hesitate to reach out.

Together, we can build a safer and more resilient digital asset ecosystem.

> **"Crypto firms can build compliance as a competitive advantage. It's no longer just about keeping up. It's about leading the industry forward."**
>
> Crypto Convergence Participant